UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/996,948	11/27/2001	Chinna Narasimha Reddy Pellacuru	50325-0607	2395

29989 7590 10/26/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
YALEW, FIKREMARIAM A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/996,948	PELLACURU, CHINNA NARASIMHA REDDY	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,9,11,12,15,17 and 20-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6,9,11,12,15,17 and 20-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The office action is in replay to an amendment filed on 08/14/2006.Claims 3-5,7-8,10,13-14,16,18-19 were previously cancelled. Claims1, 2,24,26,28,30,38 have been amended. Claims 30-45 were previously added. Claims 1-2,6,9,11-12,15,17, and 20-45 are pending.

Response to Arguments

2. Applicant's arguments with respect to claim 1-2,6,9,11-12,15,17, and 20-45 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 24,25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

5. Claims 24,25 are directed a computer-readable medium for storing instructions. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. Claims 24-25 are directed to a computer readable media that includes data signals (See specification 0097-0098). A signal does not fall within one of the four statutory classes of 101.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-2,12,15,17,20-22,24-30,34-38,42-45 rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava(US Patent No 6,684,331 B1) in view of Kocher et al(hereinafter referred as Kocher)US 6,289,455 B1.

8. As per claims 1,24,26,28: Srivastava teaches a method/apparatus/a computer-readable medium for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: receiving, at an authoritative node from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes (See col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); in response to the first request, the authoritative node storing the encryption key (See col 7 lines 38-48); the authoritative node creating and storing an association between the encryption key and the identifier(See col 9 lines 38-49;

Srivastava does not explicitly teach discloses receiving, at the authoritative node from at least one second node of the plurality of second nodes, a second receiving, from at least one second node of the plurality of second nodes, a second request to

obtain the encryption key, wherein the second request includes the identifier; in response to the second request, based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key; and the authoritative node sending the encryption key to the at least one second node for use in decrypting the encrypted data.

Kocher teaches receiving, at the authoritative node from at least one second node of the plurality of second nodes, a second receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier (See col 11 lines 15-65 and col 9 lines 7-15); in response to the second request, based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key(See col 11 lines 15-65 and col 9 lines 7-15); and the authoritative node sending the encryption key to the at least one second node for use in decrypting the encrypted data(See col 11 lines 15-65 and col 9 lines 7-15).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Kocher within Srivastava in order to provide an improved approach to distribution that enhances scalability and fault tolerance of group managers over a WAN. (See Srivastava col 4 lines 55-58)

9. As per claims 2,30,38: the combination of Srivastava and Kocher teach a method/apparatus/ a computer-readable medium wherein: the authoritative node is a trusted third party performs the steps of receiving the first request, storing the

encryption key, creating and storing the association, receiving the second request, retrieving the encryption key, and sending the encryption key (See Srivastava col 7 lines 38-48); the first request is encrypted based on a first public key that is associated with the trusted third party (See Srivastava Fig 4A step 402); the first request is signed with a first private key that is associated with the first node(See Fig 4A step 410); the first node is a router that acts as a multicast originator(See Srivastava col 8 lines 45-63); the plurality of second nodes is a plurality of routers that act as multicast receivers the trusted third party is selected from the group consisting of a certificate authority, a key distribution center, a key exchange authority, and a key exchange center(See Srivastava col 8 lines 45-63 and See Fig 4A step 410); the encryption key is selected from the group consisting of a second private key(See Srivastava Fig 4A step 410); a shared key, a pseudo-random string of bits, and a pseudo-random string of characters(See Srivastava Fig 4A step 410); and the method further comprises the computer-implemented steps of prior to sending the encryption key, encrypting the encryption key based on a second public key that is associated with the at least one second node, and signing the encrypted encryption key with a third private key that is associated with the trusted third party(See Srivastava col 7 lines 29-48 and col 8 lines 3-16).

10. As per claims 12,34,42: the combination of Srivastava and Kocher teach a method further comprising the computer-implemented steps of: storing a first list of nodes (See Srivastava col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); in response to the first request, determining whether the first node is

included in the first list of nodes: when the first node is included in the first list of nodes, performing the steps of storing the encryption key and creating and storing the association between the encryption key and the identifier, in response to the first request, storing the a second list of nodes(See Srivastava col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); In response to the second request, determining whether the at least one second node is included in the second list of nodes(See Kocher col 11 lines 15-65 and col 9 lines 7-15); and when the at least one second node is included in the second list of nodes, performing the steps of retrieving and sending the encryption key(See Kocher col 11 lines 15-65 and col 9 lines 7-15).

11. As per claim 15,35,43: the combination of Srivastava and Kocher teach a method wherein the encryption key, the identifier is an old identifier, and the association is an old association, and further comprising the steps of: in response to the first request, associating one or more criteria with the encryption key(See Srivastava col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); in response to the second request , determining based on the one or more criteria where the encryption key is valid; and when the encryption key is not valid, receiving a third request to store a new encryption key wherein the third request includes a new encryption key is used to encrypt additional data that is multicast with the new identifier to the plurality of the second nodes; in response to the third request, storing the new encryption key(See Srivastava col 7 lines 38-48); creating and storing a new association between the new encryption key and the new identifier(See Srivastava col 7 lines 38-48); receiving from at least one additional second node of the plurality of second nodes, a fourth request to

obtain the new encryption key, wherein the fourth request to obtain the new encryption key, wherein the fourth request includes the new identifier(See Srivastava col 7 lines 38-48); in response to the fourth request, based on the new identifier includes in the fourth request and the new association between the new encryption key and the new identifier, retrieving the encryption key; and sending the new encryption key to the at least one additional second node for use in decrypting the encrypted node(Kocher col 11 lines 15-65 and col 9 lines 7-15).

12. As per claims 17,36,44: the combination of Srivastava and Kocher teach a method wherein the identifier is a session identifier (see col 16 lines 55-67); the encrypted data is multicast with an originator identifier that is based on an identity of the first node (See Srivastava col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); the second request includes an unverified originator identifier (Srivastava col 7 lines 38-48 and col 7 lines 9-16); and further comprising the computer-implemented steps of: in response to the first request, associating the originator identifier with the session identifier(See Kocher col 11 lines 15-65 and col 9 lines 7-15); and in response to the second request, determining whether the unverified originator identifier is valid based on the originator identifier and informing the at least one second node whether the unverified originator is valid(See Kocher col 11 lines 15-65 and col 9 lines 7-15).

13. As per claim 20,37,45: the combination of the combination of Srivastava and Kocher teach a method wherein the identifier is selected from the group consisting of a hostname, an Internet protocol address, a media access control address, an Internet

security protocol security parameter index, a first string of pseudo-random bits, a second string of pseudo-random characters, a third string of arbitrary bits, and a fourth string of arbitrary characters (See Sruvastava col 8 lines 3-34).

14. As per claim 21,25,27,29: Srivastava teaches a method/Apparatus for encrypting a communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier (See Srivastava col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); encrypting data based on the encryption key(See col 7 lines 29-37); and multicasting the encrypted data with the identifier to one or more receiving nodes(See col 7 lines 29-37).

However Srivastava does not explicitly teaches wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.

Kocher teaches wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key (See col 11 lines 15-65 and col 9 lines 7-15).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Kocher within Srivastava in order to provide an improved approach to distribution that enhances

scalability and fault tolerance of group managers over a WAN. (See Srivastava col 4 lines 55-58)

15. As per claim 22: Srivastava teaches a method for decrypting encrypted communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: receiving from an originating node a multicast that includes encrypted data and an identifier (See col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); identifying the identifier from the multicast (See col 7 lines 38-48);

Srivastava does not explicitly teach sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data (See col 11 lines 15-65 and col 9 lines 7-15); in response to the request to the authoritative node, receiving the encryption key(See col 11 lines 15-65 and col 9 lines 7-15); and decrypting the encrypted data based on the encryption key(See col 11 lines 15-65 and col 9 lines 7-15).

However Kocher teaches sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data(See col 11 lines 15-65 and col 9 lines 7-15); in response to the request to the authoritative node, receiving the encryption key(See col 11 lines 15-65 and col 9 lines 7-15); and decrypting the encrypted data based on the encryption key(See col 11 lines 15-65 and col 9 lines 7-15).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Kocher within

Srivastava in order to provide an improved approach to distribution that enhances scalability and fault tolerance of group managers over a WAN. (See Srivastava col 4 lines 55-58)

16. Claims 6,31,39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava(US Patent No 6,684,331 B1) in view of Kocher et al(hereinafter referred as Kocher)US 6,289,455 B1 and further in view of Yung-Kao Hsu (US Patent No 5982898).

17. As per claims 6,31,39: the combination of Srivastava and Kocher teach claim 1 as recited above. Srivastava and Kocher don't explicitly teach a method/apparatus/ a computer-readable medium further comprising the computer-implemented steps of: registering a certificate that includes the encryption key and the identifier: in response to the first request, associating an expiration time with the encryption key; in response to the second request, determining based on the expiration time whether the encryption key has expired; and when the encryption key has expired, revoking the certificate.

However Yung-Kao Hsu teaches computer-implemented steps of: registering a certificate that includes the encryption key and the identifier: in response to the first request, associating an expiration time with the encryption key (col 3 lines 19-37); in response to the second request, determining based on the expiration time whether the encryption key has expired (col 3 lines 19-37); and when the encryption key has expired, revoking the certificate (col 3 lines 19-37).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Yung_Kao Hsu within

Srivastava and Kocher because it would secure communication channels by using a public key cryptosystem for authenticating a user.

18. Claims 9,11,32,33,40,41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava(US Patent No 6,684,331 B1) in view of Kocher et al(hereinafter referred as Kocher)US 6,289,455 B1 and in further view of Hardjono(U.S Patent No 6643773 B1)

19. As per claims 9,32,40: the combination of Srivastava and Kocher teach claim 1 as recited above. Srivastava and Kocher do not explicitly teach further comprising the computer-implemented steps step of: generating the encryption key based on an Internet key exchange protocol with the first node (See Hardjono col 4 lines 50-54).

However Hardjono teaches further comprising the computer-implemented steps step of: generating the encryption key based on an Internet key exchange protocol with the first node (See Hardjono col 4 lines 50-54)

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Hardjono within Srivastava and Kocher because it would enhanced the security of the system.

20. As per claims 11,33,41: the combination of Srivastava and Kocher teach claim 1 as recited above. Srivastava and Kocher do not explicitly teach further wherein: the first node uses the encryption key and internet protocol security (IPsec) to encrypt the data that is multicast; and the at least one second node decrypts the encrypted data based on the encryption key and Ipsec. However Hardjono teaches the first node uses the encryption key and internet protocol security (IPsec) to encrypt the data that is

multicast; and the at least one second node decrypts the encrypted data based on the encryption key and IPsec(See Hardjono col 4 lines 50-54).

Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to employ the teachings method of Hardjono within Srivastava and Kocher because it would enhanced the security of the system.

21. Claims 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava(US Patent No 6,684,331 B1) in view of Kocher et al(hereinafter referred as Kocher)US 6,289,455 B1.(hereinafter referred as Turtianinen) Pub. No US 2002/0059516 A1.

22. As per claim 23: Srivastava teach a method for a certificate authority to facilitate communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of: receiving, at the certificate authority from a first router that acts as a multicast originator, a first request to register an encryption key, wherein the first request includes a multicast session identifier and a list of authorized multicast receivers, and wherein the first router uses the encryption key to encrypt data and multicasts the encrypted data with the multicast session identifier to a plurality of second routers that act as multicast receivers(See col 7 lines 38-48 and col 7 lines 9-16 and Fig 3 step 103,Fig 1 step 103,113); in response to the first request, the certificate authority creating and storing a multicast session certificate that includes the encryption key, the multicast session identifier, and the list of authorized multicast receivers(See col 7 lines 38-48);

Srivastava does not explicitly teach receiving, at the certificate authority from at least a particular second router of the plurality of second routers, a second request to obtain the encryption key, wherein the second request includes the multicast session identifier; in response to the second request, determining whether the particular second router is included in the list of authorized multicast receivers; when the particular second router is included in the list of authorized multicast receivers, based on the multicast session identifier included in the second request and the multicast session certificate, the certificate authority retrieving the encryption key; and the certificate authority sending the encryption key to the particular second router for use in decrypting the encrypted data.

However Kocher teaches receiving, at the certificate authority from at least a particular second router of the plurality of second routers, a second request to obtain the encryption key, wherein the second request includes the multicast session identifier (See col 11 lines 15-65 and col 9 lines 7-15; in response to the second request, determining whether the particular second router is included in the list of authorized multicast receivers (See col 11 lines 15-65 and col 9 lines 7-15); when the particular second router is included in the list of authorized multicast receivers, based on the multicast session identifier included in the second request and the multicast session certificate, the certificate authority retrieving the encryption key; and the certificate authority sending the encryption key to the particular second router for use in decrypting the encrypted data(See col 11 lines 15-65 and col 9 lines 7-15). Therefore it would have been obvious for one ordinary person in the art at that time the invention was made to

employ the teachings method of Kocher within Srivastava in order to provide an improved approach to distribution that enhances scalability and fault tolerance of group managers over a WAN. (See Srivastava col 4 lines 55-58)

The combination of Srivastava and Kocher do not explicitly teach encrypt data based on IPsec. However Turtiainen teaches use of IPsec in multicast system (0012-0014,0033). Therefore it would be obvious to one having ordinary skill in the art at the invention was made to employ the teachings method of Tuntianinen with the system of Srivastava and Kocher in order to achieve secure communication among multicast group communication.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser,can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
10/20/06
FA

Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/22/06